Health Matrix: The Journal of Law-Medicine

Volume 28 | Issue 1

2018

Health Care Held Ransom: Modifications to Data Breach Security & the Future of Health Care Privacy Protection

Ryan M. Krisby

HEALTH CARE HELD RANSOM: MODIFICATIONS TO DATA BREACH SECURITY & THE FUTURE OF HEALTH CARE PRIVACY PROTECTION

Ryan M. Krisby†

CONTENTS

† J.D. Candidate, 2018, Case Western Reserve University School of Law; B.A. University of Dayton; winner of the Health Matrix Outstanding Note of the Year (2017). I would like to thank Professor Sharona Hoffman for her guidance and invaluable insight throughout the process of writing this Note. I would also like to thank my peers at Health Matrix, for keeping me sane all the while. Finally, I would like to thank the following: Mom and Dad (for your bottomless supply of love and support) and Jessica Edelstein (for the humbling reminder that I am not as cool as I sometimes believe myself to be).

I. INTRODUCTION

> *"Hospital and healthcare software security can always be marginally improved, but if we want to lower the risk of healthcare security breaches, we need to take a very different approach. Only marginal improvements can be made by investing in more of the same resources in the problem, and the [return on investment] has diminishing marginal returns. A better approach is to understand the root causes at the core of healthcare security breaches."*
>
> —Ron Avignone[1]

On February 5, 2016, Hollywood Presbyterian Medical Center in Los Angeles, California, was held hostage when an anonymous hacker infiltrated its information systems.[2] The security breach shut down the hospital's entire information system—the computerized databases storing all the hospital's electronic information—sending the hospital offline for more than a week.[3] Doctors and other hospital employees were unable to access any electronic documents, patient data, or even e-mail.[4] The cybercriminal had somehow pierced the security of the Medical Center, and once inside was able to encrypt all of the files on the Center's information system.[5] This resulted in the data being "translated" into a different form, unreadable to anyone without a specific password.[6] Without that password, the hospital was locked out of

1. Ron Avignone is founder of Giva, a California-based tech company that centers around help desk applications. Ron Avignone, *Ethical hacking a vital necessity to fight against healthcare ransomware*, MED. ECON. (April 27, 2016), http://medicaleconomics.modernmedicine.com/medical-economics/news/ethical-hacking-vital-necessity-fight-against-healthcare-randsomeware.

2. *See* Trevor Mogg, *Hollywood Hospital Pays $17,000 to Ransomware Hackers*, DIGITAL TRENDS (Feb. 18, 2016), http://www.digitaltrends.com/computing/hollywood-hospital-ransomware-attack/.

3. *Id.*

4. *Id.*

5. *Id.*

6. *What is Data Encryption?*, DIGITAL GUARDIAN https://digitalguardian.com/blog/what-data-encryption (last updated July 27, 2017) (explaining that the process of encryption "translates" plaintext—readable data—into ciphertext, which is almost entirely unreadable compared to its prior

accessing any data on its system. Unfortunately for the hospital, a restoration of access to its data had a price: $17,000 in the form of bitcoin, a digital currency.[7]

Hollywood Presbyterian Medical Center eventually relented and paid the $17,000 ransom.[8] Allen Stefanek, the Chief Executive of the Medical Center, explained that paying the sum demanded by the hacker was "[t]he quickest and most efficient way to restore [its] systems and administrative functions."[9] Although Stefanek attempted to downplay the breach by announcing that no patient information or hospital records were compromised,[10] the fact still remains that an unknown cybercriminal infiltrated the Medical Center's cybersecurity and gained access to the sensitive health information of its patients. Although the hacker decided to encrypt the data files and demand a ransom, it could also have decided to simply steal the information outright.[11]

Today, patients find themselves in a digital economy.[12] Industries have been swept into the current of the data-driven world and have been forced to adapt accordingly to survive.[13] Healthcare is no different. The trend of patient-centered "on demand" services has pushed healthcare providers into the digital age of integrating technology into the practice of medicine, both in the solutions they offer patients and the administration of healthcare organizations.[14] Entrance into the

---

form). This process is described in greater detail in Part II, section C of this Note.

7. Danny Yadron, *Los Angeles Hospital Paid $17,000 in Bitcoin to Ransomware Hackers*, The Guardian (Feb. 17, 2016), https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center.

8. *Id.*

9. Richard Winton, *Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating*, L.A. TIMES (Feb. 18, 2016), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

10. *Id.*

11. *See, e.g.,* Chris Stobing, *Ransomware is the New Hot Threat Everyone is Talking About; What do You Need to Know?*, DIGITAL TREND (June 6, 2015), http://www.digitaltrends.com/computing/what-is-ransomware-and-should-you-be-worried-about-it/ ("[Ransomware] offered a simple, and reliable revenue stream that the underground market could capitalize on to fund other, less-profitable operations.").

12. *See* Lindsey Anderson & Irving Wladawsky-Berger, *The 4 Things It Takes to Succeed in the Digital Economy*, HARV. BUS.REV. (Mar. 24, 2016), https://hbr.org/2016/03/the-4-things-it-takes-to-succeed-in-the-digital-economy.

13. *Id.*

14. *See* Dennis Bonilla, *Five Tips You Need to Ease Patient Concerns in the Digital Age*, MODERN HEALTHCARE http://www.modernhealthcare.com

digital realm comes a host of cybernetic threats. Unlike many other industries, however, healthcare providers control troves of highly sensitive information, a fact of which their patients are hyperaware.[15] As a result, healthcare providers have a target on their back.[16] Ransomware is a new menace on the cyber-threat scene and has recently begun targeting hospitals and other healthcare providers. And while Hollywood Presbyterian Medical Center's attack garnered a lot of attention, it was not the first of its kind and certainly will not be the last.

Early in February 2016, Methodist Hospital in Henderson, Kentucky declared a "state of emergency" when a hacker prevented the hospital from accessing patient files.[17] The following month, MedStar Health—a health system that operates ten hospitals and over 250 outpatient facilities—was attacked and forced to shut down its entire records database.[18] Between October 2015 and January 2017, an unauthorized user accessed patient information held by Verity Medical Foundation.[19] The compromised information included the names, birth dates, medical record numbers, addresses, and credit card numbers of more than 9,000 individual patients.[20] Verity failed to detect the breach until January 6, 2017.[21] On January 3, 2017, Emory Healthcare—an Atlanta-based hospital system—discovered a compromise of approximately 80,000 records of patients who used its online

/article/20161101/SPONSORED/161109984/five-tips-you-need-to-ease-patient-concerns-in-the-digital-age (last accessed Mar. 8, 2017).

15. *Id.* ("Our consumers are hyperaware of the sensitive information included in their health records.").

16. *See* Akanksha Jayanthi, *16 Latest Healthcare Data Breaches, Security Incidents*, HEALTH IT & CIO REV. (Sept. 26, 2016), http://www.beckershospitalreview.com/healthcare-information-technology/16-latest-healthcare-data-breaches-security-incidents.html (reporting sixteen healthcare data breaches or incidents occurring within a single four-week period).

17. Kim Zetter, *Why Hospitals are the Perfect Targets for Ransomware*, WIRED (Mar. 30, 2016), available at: https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.

18. John Woodrow Cox, Karen Turner & Matt Zapotosky, *Virus infects MedStar Health system's computers, forcing an online shutdown*, WASH.POST (Mar. 28, 2016), https://www.washingtonpost.com/local/virus-infects-medstar-health-systems-computers-hospital-officials-say/2016/03/28/480f7d66-f515-11e5-a3ce-f06b5ba21f33_story.html.

19. *Verity Health System Notifies Patients of Data Incident*, BUSINESS WIRE (Feb. 6, 2017), http://www.businesswire.com/news/home/20170206005855/en.

20. *Id.*

21. *Id.*

appointment system.[22] As illustrated here, by a mere handful of breach examples, the cybersecurity of many healthcare providers is inadequate.

These attacks continue to happen despite the number of requirements healthcare providers must meet to protect the sensitive information of their patients. Federal regulation regarding the protection of patient privacy is rooted in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its subsequent regulations.[23] In particular, the Security Rule implemented by the United States Department of Health and Human Services (HHS) in accordance with HIPAA governs the safeguards healthcare providers and other covered entities must establish for the protection of electronic patient data.[24] While the Security Rule promulgates many safeguards for the protection of patient data, it still falls short in light of new cyber-threats, such as ransomware. Data breaches continue to happen, and they continue to happen on a gigantic scale.

In sum, current federal data breach security regulation fails to adequately protect patient data. In light of recently developing threats to electronic personal health data, HIPAA's Security Rule should be modified to provide more stringent protections, while maintaining the flexibility and scalability promulgated by HIPAA.

Part II of this Note provides background on data breach security under HIPAA. In particular, it describes the federal regulations for the protection of electronic health data and explains ransomware and the threat it poses to data security. Part III of this Note highlights the inadequacies of federal data breach regulations and proposes modifications that address these inadequacies both generally and concerning ransomware more specifically. Finally, Part IV discusses recent actions by the Federal Trade Commission ("FTC") and how its enforcement actions provide an impetus for healthcare organizations to carry out data security modifications.

II. BACKGROUND

A. HIPAA & Risk

HIPAA is in large part about risk. Risk is "used colloquially to suggest that an action or decision may lead to a negative outcome."[25]

22. Rachel Arndt, *Emory Healthcare Cyberattack Affects 80,000 Patient Records*, MODERN HEALTHCARE (Mar. 2, 2017), http://www.modernhealthcare.com/article/20170302/NEWS/170309983/emory-healthcare-cyberattack-affects-80000-patient-records.

23. *See generally* 42 U.S.C. § 1320d et seq. (2016).

24. *See generally* 45 C.F.R. §§ 160 & 164 (2016).

25. Kristin N. Johnson, *Managing Cyber Risks*, 50 GA. L. REV. 547, 556 (2016) (citing GEOFFREY PARSONS MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 535 (2014)).

More accurately, however, risk simply means uncertainty.[26] The cause of this uncertainty may stem from a variety of factors, including human error, flaws in the organizational system, technical system failures, or a multitude of external factors.[27] In respect to only the uncertain *negative* outcomes, risk management can be characterized as the avoidance or limiting of these negative risks.

The following visualization of structural risk illustrates the relationship between risk factors and potential negative outcomes:

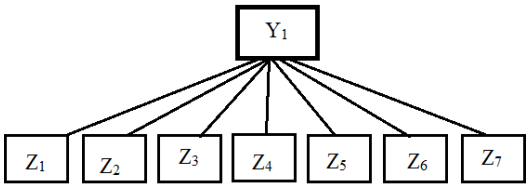


Figure 1.[28]

Z_1, Z_2, Z_3, . . . Z_7 represent several kinds of unfavorable events. Y_1 is an undesired outcome. Event Y_1 will occur if at least one of any of the events in the set Z_1, . . . ,Z_7 occur. Assuming any event in Z_1, . . . ,Z_7 either will, or will not, occur, any person or organization wanting to eliminate the occurrence of Y_1 will want to in some way limit the set of events leading to that outcome.[29] Take, for example, a ship carrying bottles of wine from a vineyard in France to a wine distributor in the United States. The undesired outcome of this voyage is the wine not making it safely to the wine distributor in the U.S. A series of events may lead to the wine not making it stateside: the wine bottles may be damaged, the cargo may be lost at sea, the ship may strike a leak and sink, or the ship may be commandeered by pirates. The seller-vineyard—in order to avoid this undesired outcome—would enforce certain requirements on his carrier to limit the set of events that would lead to it: properly storing and fastening the cargo of wine

26. *Id.* ("Risk simply describes an element of uncertainty or the chance for a range of possible outcomes.").

27. Ekaterina Karaseva, *Ability of Logical and Probabilistic Model for Operational Risk Management*, 11 Reliability: Theory & Application 23, 23 (Sept. 2016).

28. *See id.* at 24 for the original model ("Structural model of operational risk for first business line.").

29. *Id.* at 25 (discussing the model and explaining the relationship between outcome Y and the Z-set of events).

bottles, ensuring any holes in the ship are sealed to not let in water, and avoiding routes known for pirate attacks.[30]

Similarly, HIPAA imposes many requirements on healthcare providers to avoid the undesired outcome of unauthorized access of patients' personal health information. Like the carrier of the wine, healthcare providers carry the precious information of their patients. And, like the seller-vineyard, HIPAA is deeply concerned with how that "cargo" is handled. There are *a lot* of requirements promulgated under HIPAA.[31] These requirements aim to address vulnerabilities that are commonly exploited and cause an undesired outcome.[32] While the requirements under HIPAA address a wide variety of risk factors, the section that specifically provides for the protection of electronic health information is known as the Security Rule.[33]

B. HIPAA's Security Rule

Regulations promulgated by HHS under HIPAA are commonly referred to as the Privacy and Security Rules.[34] HIPAA was amended in 2009 by the Health Information Technology for Economic and Clinical Health Act (HITECH)[35] and updated in January 2013 with HHS's publication of the Omnibus Final Rule.[36] While the Privacy Rule protects all "individually identifiable health information,"[37] the Security Rule protects only electronic protected health information (ePHI) and is therefore the basis for federal data breach security regulation.[38]

30. The facts of this hypothetical are inspired by the facts of Rheinberg-Kellerei GMBH v. Vineyard Wine Co., 281 S.E. 2d 425 (1981) in which a large shipment of wine lost at sea resulted not only in a contract dispute, but a sea full of drunken fish.

31. *See* 42 U.S.C. § 1320d (2006).

32. *HIPAA for Professionals*, U.S. DEP'T OF HEALTH & HUM. SERV. https://www.hhs.gov/hipaa/for-professionals/index.html (last updated on June 16, 2017) ("To improve the efficiency and effectiveness of the health care system . . . [HIPAA] required HHS to adopt national standards for electronic health care transactions . . . ").

33. 45 C.F.R. §§ 160 & 164 (2016).

34. *See* 45 C.F.R. §§160, 162, 164 (2016).

35. 42 U.S.C. §17935 (2016).

36. *See* General Administration Requirements, 45 C.F.R. §160 (2016) and Security and Privacy, 45 C.F.R. § 164 (2016).

37. *See* 45 C.F.R. § 160.103 (2016).

38. *See* 45 C.F.R. § 164.306(a)(1) (2016).

ePHI is electronically stored, personally identifiable health information collected from an individual.[39] These data are stored in health information systems (HIS) around the globe "in hospitals, research centers, and diagnostic laboratories."[40] The Security Rule divides the risks that threaten to exploit the vulnerabilities of HISs into three categories: physical, administrative, and technical.[41] These risks would form the set $Z_1, \ldots, Z_7$ in Figure 1 above.[42] For example, if ePHI were stored on a single computer, a physical risk would be the probability of someone burglarizing the computer and the data on it.[43] The Security Rule establishes three categories of safeguards—physical, administrative, and technical[44]—which all work together to limit the probability of the vulnerabilities in HISs being exploited.[45]

Each security standard includes a variety of implementation specifications, which are designated as either "required" or "addressable."[46] Although healthcare organizations must adhere to the Security Rule's standards, they are not bound to observe every single implementation specification described within the standards.[47] Healthcare providers *must* implement the implementation specifications labeled as "required." Meanwhile, implementation specifications labeled as "addressable" provide healthcare organizations with some discretion.

39. *See Integrating Privacy & Security Into Your Practice*, HEALTH IT,https://www.healthit.gov/providers-professionals/ehr-privacy-security/practice-integration (last updated Apr. 13, 2015).

40. Shahidul Islam Khan, Abu Sayed & Latiful Hoque, *Digital Health Data: A Comprehensive Review of Privacy and Security Risks and Some Recommendations*, 24 COMPUTER SCI. J. OF MALDOVA 273, 274 (2016).

41. *See* 45 C.F.R. § 160 (2016); *see also* 45 C.F.R. § 164, subparts A and C (2016) and *The Security Rule*, HHS.GOV https://www.hhs.gov/hipaa/for-professionals/security/index.html (last updated May 12, 2007).

42. *See* Karaseva, *supra* note 27, at 24 (Figure 1 above).

43. *See, e.g.,* 45 C.F.R § 164.310(a)(1) (2016) (Physical safeguards, which protect against physical risks, include facility access control, which implies "policies and procedures to limit physical access to its electronic information systems.").

44. *See Summary of the HIPAA Security Rule* ,U.S. DEP'T OF HEALTH & HUM. SERV., http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last updated July 26, 2013) [hereinafter U.S. DEP'T OF HEALTH & HUM. SERV.].

45. *See id.*

46. *For Professionals: FAQ, What is the Difference Between Addressable and Required Implementation Specifications in the Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERV., https://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html (last updated July 26, 2013).

47. *See id.*

"Addressable" does not mean "optional."[48] Rather, a healthcare provider may assess whether the implementation specification is reasonable, and if not, then it is permitted to implement a more appropriate alternative measure than the "addressable" specification.[49] The Handbook for HIPAA-HITECH Security published by the American Medical Association describes "addressable" specifications as "situational."[50]

1. Physical Safeguards

Physical safeguards are requirements related to "buildings and equipment"[51] and the risks posed by "natural and environmental causes," and unauthorized intrusion from unsanctioned human physical access.[52] A crucial note here is that "data back up and storage" is labeled as "addressable."[53] Under this implementation specification, healthcare organizations should "create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."[54] The "addressable" provisions also include facility security planning and access control and validation, both of which are promulgated with very broad regulatory language.[55]

2. Administrative Safeguards

Administrative safeguards are the "nontechnical measures that an organization's management establishes regarding acceptable employee conduct, personnel procedures, and correct technology usage within the enterprise."[56] The most important standard required under the administrative safeguards is the security management process.[57] Organizations should assess potential risks to their data security and

48. U.S. DEP'T OF HEALTH & HUM. SERV., *supra* note 44.

49. 45 C.F.R. § 164.306(d) (2016). *See also* 45 C.F.R. § 164.308(a)(1)(ii) (2016) (explaining that execution of the Security Rule is driven in large part by the risk analysis and management instituted in the administrative safeguards.).

50. MARGARET AMATAYAKUL, HANDBOOK FOR HIPAA-HITECH SECURITY 84 (2d ed. 2013) ("You must address these specifications, but you may do so according to your own situation.").

51. 45 C.F.R. § 164.304 (2016) (defining "physical safeguards").

52. *Id.*; *see also* Mike Jerbic & Stephen Wu, *The Security Rule*, *in* A GUIDE TO HIPAA SECURITY AND THE LAW 62 (Stephen S. Wu, ed., 2007).

53. 45 C.F.R. § 164.310(d)(2)(iv) (2016).

54. *Id.*

55. *See* 45 C.F.R. § 164.310(a)(2)(ii)–(iii) (2016).

56. Jerbic & Wu, *supra* note 52, at 27-28; *see also* 45 C.F.R. § 164.304 (2017) (defining "administrative safeguards").

57. *See* 45 C.F.R. § 164.308(a)(1)(i) (2016).

"implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."[58] Two addressable implementation specifications under this section are "access authorization" and "access establishment & modification."[59] Under these provisions, a healthcare provider is encouraged to have in place policies that establish and limit the level of access to data within its HIS.[60] Also addressable are the specifications under the category Security Awareness and Training.[61] This means that healthcare providers have a lot of discretion on how they run as a top-to-bottom organization, including who within the organization has access to what within the organization's HISs.[62] Despite employee negligence being noted as a major contributing factor to data security problems,[63] healthcare organizations are given this broad discretion on the authorization-related safeguards under HIPAA.

3. Technical Safeguards

Technical safeguards are flexible requirements for the operations of HISs that "store, process, or transmit ePHI."[64] Addressable safeguards in this section include the specification that healthcare organizations should "implement a mechanism to encrypt and decrypt electronic protected health information."[65] This provision does not provide any other information, including differentiating between data-at-rest and data-in-motion, or a minimum level of encryption.[66] In other words, the technical safeguards mandated by HIPAA do not distinguish when data

58. 45 C.F.R. § 164.308(a)(1)(ii)(B) (2007).

59. 45 C.F.R. § 164.308(a)(4)(ii)(B)–(C) (2007).

60. *Id.*

61. *See* 45 C.F.R. § 164.308(a)(5)(i)–(a)(5)(ii)(D) (2007).

62. *See, e.g., HIPAA Security Series: Part 2*, U.S. DEP'T OF HEALTH & HUM. SERV., 9 (March 2007), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf.

63. *See* Ponemon Institute, *Third Annual Benchmark Study on Patient Privacy & Data Security*, 9 (2012) (the study found "insider negligence" one of the central factors in a significant portion of data breaches); *see also* Lucy L. Thomson, *Health Care Data Breaches and Information Security*, *in* HEALTH CARE IT: THE ESSENTIAL LAWYER'S GUIDE TO HEALTH CARE INFORMATION TECHNOLOGY AND THE LAW 255 (Arthur Peabody, Jr., ed., 2013) ("Responses . . . attributed [rise in data breaches] to a lack of technologies, resources, and trained personnel.").

64. *See* Jerbic & Wu, *supra* note 52, at 76; *see also* 45 C.F.R. § 164.304 (2017) (defining "technical safeguards" as "the technology and the policy and procedures for its use that protect electronic health information and control access to it.").

65. 45 C.F.R. § 164.312(a)(2)(iv) (2007).

66. *Id.*

are "moving" across a network—be it private or public—and when they are stored in some form (or "at rest").[67] Encryption is mentioned again in § 312(e)(2)(ii).[68] Data should be encrypted whenever the healthcare organization "deem[s] [it] appropriate."[69] Across the board, the required minimum level of technical safeguards in place to protect HISs and ePHI from cyber-threats are far too lax. This has inevitably led threats such as ransomware to wreak havoc on the healthcare industry.

C. Ransomware

1. Encryption

Ransomware employs encryption to prey on unsuspecting persons. Encryption is "the transformation of data into a form unreadable by anyone without a secret decryption key."[70] The purpose of encryption is privacy: even someone with access to the encrypted data ("ciphertext") is unable to discern the data in readable form ("plaintext").[71] There are two types of encryption, or cryptography: symmetric key cryptography and public key cryptography.[72] In symmetric key cryptography, the sender and receiver use the *same* secret key to encrypt and decrypt the data.[73] Public key cryptography uses a pair of keys: a public and a private key.[74] The public key is shared between both parties, while both sender and receiver have a unique private key.[75] The public key is used to encrypt the data, but can only be decrypted back into plaintext with the corresponding private key. For example: A, B, and C want to encrypt the messages they send amongst each other. A, B, and C's public keys are openly known. A and C can encrypt a message with the B-public-key. Only B, however, can decrypt and read the message using B's secret, private key.

67. *See Regulation and Standards: Where Encryption Applies*, SANS INST., 2 (Nov. 2007), https://www.sans.org/reading-room/whitepapers/analyst/regulations-standards-encryption-applies-34675 ("*Data in transit* is commonly delineated into two primary categories—data that is moving across public or 'untrusted' networks, such as the Internet, and data that is moving within the confines of private networks.").

68. 45 C.F.R. § 164.312(e)(2)(ii) (2007).

69. *Id.*

70. *Encryption FAQ*, STAN. UNIV., https://cs.stanford.edu/people/eroberts/cs181/projects/1995-96/clipper-chip/encyptfaq.html (last accessed Mar. 10, 2017).

71. *Id.*

72. *Id.*

73. *Id.* (Author uses the term "secret key cryptography," but the concepts are synonymous.).

74. *Id.*

75. *Id.*

Ransomware uses hybrid encryption, combining the two cryptographies to create an *asymmetrical* cryptosystem.[76] In this cryptosystem, the public key cryptosystem is used for key encapsulation and a symmetric key is used for data encapsulation.[77] Data is encrypted using a randomly-generated symmetric key.[78] This symmetric key is subsequently encrypted using a public key where one party has the corresponding private key.[79] The party with the private key decrypts the symmetric key using the private key.[80] The recovered symmetric key can then be used to decrypt the data back into plaintext.

2. Ransomware Attacks

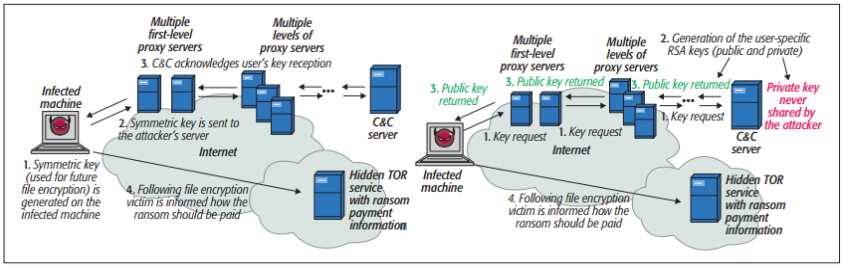


Figure 2.[81]

Ransomware is malware that carries out a cryptoviral extortion attack, in which the data of a target computer or information system is virtually "held hostage" until a ransom is paid. It is one of the fastest growing cybersecurity threats and has recently become a terror to healthcare providers.[82] The worst part about the torrent of ransomware

76. *See* Jonathan Katz, *Lecture 4*, *Advanced Topics in Cryptography*, UNIV. MD., 4-1 (Feb. 5, 2004), *available at*: https://www.cs.umd.edu/~jkatz/gradcrypto2/NOTES/lecture4.pdf.

77. *See id.*

78. *See id.*

79. *Id.* ("A hybrid encryption scheme uses public-key encryption to encrypt a random symmetric key, and then proceeds to encrypt the message with that symmetric key.").

80. *See id.*

81. Krzysztof Cabaj & Wojciech Mazurczyk, *Using Software-Defined Networking for Ransomware Mitigation: The Case of Cryptowall*, 30 IEEE NETWORK 14, 15 (Nov. 2016). (Figure used in authors' explanation of ransomware ("Symmetric (left) and asymmetric (right) crypto ransom-ware"). The asymmetric model is more commonly used today to extort victims.).

82. *See* Kim Zetter, *Why Hospitals are the Perfect Targets for Ransomware*, WIRED (Mar. 30, 2016), https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.

attacks: there does not seem to be a sufficient answer to this threat.[83] In fact, the Assistant Special Agent in charge of the FBI's Boston Cyber & Counterintelligence office has noted that "[t]he ransomware is *that* good."[84] In 2015, the FBI stated it may be easiest for victims of ransomware attacks to "just pay the ransom," as efforts to solve the data-encrypting algorithms after a breach occurred were essentially useless.[85] So, how exactly does ransomware work?

Ransomware functions by "[p]reying on human error."[86] Cybercriminals who employ ransomware typically infect victims through some form of social engineering that lures unsuspecting victims into unknowingly opening their system to malware.[87] The cybercriminals behind ransomware—often disguising their malware as something far less malicious—lure victims into activating the program,[88] which then hijacks and encrypts the victim's system.[89] Methods include phishing, spam, drive-by-download, or any method that disguises a malware's payload as a legitimate file. One example is a lawyer receiving a polished and well-crafted e-mail inquiring about employment at his firm. The e-mail included an attached resume in the form of a Microsoft Word document, which activated the ransomware when the lawyer clicked to open it.[90] Ransomware may also spread on its own by using gaps in a computer system to access and encrypt the data without any interaction on the part of the victim.[91]

---

83. Paul, *FBI's Advice on Ransomware? Just Pay the Ransom.*, THE SEC. LEDGER (October 22, 2015), https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/.

84. *Id.* (emphasis added).

85. *Id.*

86. Mohamad Ali, *Is Your Company Ready for a Ransomware Attack?*, HARV. BUS. REV. (Oct. 3, 2016), https://hbr.org/2016/10/is-your-company-ready-for-a-ransomware-attack.

87. Cabaj & Mazurczyk, *supra* note 81.

88. There are multiple brands of ransomware; ransomware simply refers to the species of cyber-threat. *See* Ondrej Krahel, *Ransomware—A Sneaky, Dangerous Cyber Threat*, CSO (Feb. 15, 2017), https://www.csoonline.com/article/3170196/security/ransomware-is-a-sneaky-dangerous-cyber-threat.html.

89. Ali, *supra* note 86.

90. Steve Strauss, *Why Your Small Business Needs to Care About Ransomware*, FIGHT RANSOMWARE, https://fightransomware.com/ransomware-articles/small-business-needs-concerned-ransomware/ (last visited Oct. 22, 2017).

91. *See* Ali,*supra* note 86; *see also* Cammy Harblson, *New Ransomware Installers Can Infect Computers Without Users Clicking Anything, Say Researchers*, DIGITAL TIMES (Mar. 29, 2016), http://www.idigitaltimes

Once a victim's device or system has been infiltrated by the cybercriminal's malware, the malware encrypts the victim's data using a randomly-generated symmetric key.[92] This locks the system, including personal cloud storage services.[93] The malware uses a public key to encrypt the symmetric key, creating an asymmetric cryptosystem.[94] A victim's computer then displays a ransom message, demanding some fee to gain access to data. The victim pays the ransom, and sends the fee along with the encrypted symmetric key.[95] The cybercriminal uses a private key to decrypt the symmetric key and sends the key back to the victim, who can then use it to re-gain access to their system.[96]

3. The Current State of Data Security in Healthcare

The United States is the country most widely impacted by ransomware attacks.[97] As of 2013, data breaches in healthcare accounted for 45 percent of all data security breaches.[98] In 2016 alone, healthcare data breaches comprised 35 percent of all breaches, a figure that the business sector has only recently eclipsed.[99] In 2016, 44 perecnt of healthcare organizations participating in a Ponemon Institute Study reported that ransomware was their greatest cyber-related concern.[100]

.com/new-ransomware-installers-can-infect-computers-without-users-clicking-anything-say-522756.

92. Cabaj & Mazurczyk, *supra* note 81.

93. Ali, *supra* note 86.

94. Cabaj & Mazurczyk, *supra* note 81.

95. *See* Kevin Savage, et al., *The Evolution of Ransomware*, SYMANTEC SECURITY RESPONSE, 22–23 (Aug. 6, 2015), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf (The payments usually go through several proxies and is made in the hard-to-trace currency bitcoin.).

96. Cabaj & Mazurczyk, *supra* note 81.

97. Savage et al., *supra* note 95, at 34 (making up 54% of all binary-based ransomware attacks among the world's twelve wealthiest countries).

98. *Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RES. CTR. (Jan. 19, 2017), http://www.idtheftcenter.org/2016databreaches.html.

99. *Id.* Although this is somewhat of an anomaly in recent years, even with the business industry having high profile data breach cases such as Target and Home Depot. *See* Kevin McCoy, *Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers*, USA Today (May 23, 2017), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/; *see also* Jeff John Roberts, *Home Depot to Pay Banks $25 Million in Data Breach Settlement*, Fortune (Mar. 9, 2017), http://fortune.com/2017/03/09/home-depot-data-breach-banks/.

100. Ponemon Institute, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*, 13 (May 2016). Denial of Service (DoS) attacks were

Documents containing the most damaging and sensitive patient information—medical files and billing and insurance records—were most likely to be successfully targeted by cybercriminals.[101] Of the surveyed healthcare organizations, 64percent reported compromised medical files, and 45 percent reported breached billing and insurance records.[102] This rate represented an increase from previous years. Healthcare organizations have always been particularly vulnerable, and security has never been more important.

Dangers to healthcare data security come from two sources: the data security software design and the persons who "manipulate the [health IT] systems."[103] A study conducted by the Pennsylvania Patient Safety Authority that examined electronic health record-related incidents between 2004 and 2012 concluded that "[t]he majority of EHR-related reports involved [human error]."[104] Human error, in particular, is a major factor in healthcare-related breaches.

According to HHS, between 2009 and 2013, the top causes of data breaches affecting 500 or more individuals were: improper disposal (5%), hacking/IT incident (6%), loss (11%), unauthorized access (20%), and theft (54%).[105] In 2015, breaches affecting 500 or more individuals totaled 253, with a loss of 112 million personal healthcare records.[106] Also, in 2015 "hacking/IT incident" and "unauthorized access"

reported by 48% of covered entities as their greatest concern. DoS attacks have been used by cybercriminals in conjunction with ransomware breaches. *See, e.g.,* Ricci Dipshan, *Danger Ahead: 3 New Ransomware Developments in 2016*, LAW TECH. NEWS (May 31, 2016), http://www.legaltechnews.com/id=1202758839457/Danger-Ahead-3-New-Ransomware-Developments-in-2016-?slreturn=20170827111230.

101. Ponemon Institute, *supra* note 100, at 21.

102. *Id.*

103. *See* Arthur E. Peabody Jr., *Safety Risks Associated with EHRs: How Real?*, *in* HEALTH CARE IT: THE ESSENTIAL LAWYER'S GUIDE TO HEALTH CARE INFORMATION TECHNOLOGY AND THE LAW 243-44 (2013).

104. Erin Sparnon & William M. Marella, *The Role of the Electronic Heath Record in Patient Safety Events*, 9 Penn. Patient Safety Adv., 113, 113-121 (Dec. 2012), http://patientsafety.pa.gov/ADVISORIES/documents/201212_113.pdf; *see also* Peabody, *supra* note 103.

105. MARGRET AMATAYAKUL, HANDBOOK FOR HIPAA-HITECH SECURITY 11-12 (2d ed. 2013) (analyzing the data from U.S. DEP'T OF HEALTH & HUM. SERV., OCR, Breaches Affecting 500 or More Individuals (last visited Oct. 29, 2016), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

106. *See* Dan Munro, *Data Breaches in Healthcare Totaled Over 112 Million Records in 2015*, FORBES (Dec. 31, 2015), http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#1b03d7137fd5; *see also* U.S. DEP'T OF HEALTH & HUM. SERV., OCR, Breaches Affecting 500 or More Individuals, *supra* note 105.

composed a majority of the larger security breaches.[107] 2016 saw a 320 percent increase in breaches affecting 500 or more individuals caused by hacking/IT incidents.[108] Therefore, while technology-driven breaches caused a significant portion of the attacks, almost all breaches were caused in some way by to human error.[109] This indicates changes in mandated administrative practices may result in better data security.

The level of compliance with security measures across the healthcare industry is anything but perfect. Between April 2003 and December 2017, the Office of Civil Rights (OCR) of HHS investigated 37,023 complaints of HIPAA violations.[110] Of those investigations, 25,637 resulted in corrective action, while the remainder found "no violation."[111] That means the OCR found that violations existed in over 68 percent of the investigated complaints.[112] While 37,023 is a drop in the bucket compared to the number of total healthcare organizations in the United States, the percentage of investigated organizations who were not in compliance is startling. The synchrony of heightened threats of ransomware and other data security attacks with the lack of compliance in the healthcare industry results in a huge potential for devastating consequences when data breaches do in fact occur.

In particular, ransomware shapes a large swath of the current data security landscape. In 2016 alone, ransomware attacks accumulated approximately $1 billion in ransom payments worldwide.[113] The general perception across the healthcare industry is that ransomware attacks will increase throughout 2017.[114] So far, this feeling has turned out to be true. In May 2017, the world saw the "biggest ransomware attack in

107. *See* Munro, *supra* note 106; *see also Understanding the Depth of the Global Ransomware Problem*, MALWAREBYTES, 10_(Aug. 2016), https://www.malwarebytes.com/surveys/ransomware/?aliId=13242065. (The percent distribution was different, and the category of hacking/IT incident was split into several categories, including "e-mail phishing" and "ransomware.").

108. REDSPIN, *Breach Report 2016: Protect Health Information (PHI)*, CYNERGISTEK 5 (Fed. 2017), https://www.redspin.com/resources/download/breach-report-2016-protected-health-information-phi/ [hereinafter REDSPIN].

109. *Id.* at 17.

110. *See Numbers at a Glance, Health Information Privacy*, U.S. DEP'T OF HEALTH & HUM. SERV.https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/numbers-glance/index.html (last updated July 31, 2017).

111. *Id.*

112. *Id.*

113. REDSPIN, *supra* note 108, at 10.

114. *Id.*

history."[115] Although the attack was widespread from Spain to Japan, it hit England particularly hard, where is sent the National Health Service (NHS) into flight or fight response.[116] Hospitals and other healthcare organizations across London and northern England were forced to "revert to pen and paper" in many instances.[117] Some organizations even had their staff using personal mobile devices in the place of encrypted systems.[118] Now, more than ever, ransomware is a threat and necessitates action on the regulatory level.

4. The Cost of Ransomware and Other Cyber-threats

Healthcare organizations are potential cash cows for cybercriminals. Across the healthcare industry in 2015 alone, the cost of data breaches was $363 per record.[119] This is compared to $154 per record cost across all other industries.[120] Indeed, the price of not protecting the data on HISs is steep. Over a two-year period, economic losses to healthcare organizations from data security breaches ranged from less than $10,000 to well over $1 million.[121] The price of data breaches has only been on the rise. More recently, the cost of data breaches to healthcare organizations has increased to $380 per record.[122] Because of the increasing value of data, the costs of data breaches are expected to

115. *See* Henry Bodkin, et al., *Government Under Pressure After NHS Crippled in Global Cyber Attacks as Weekend of Chaos Looms*, THE TELEGRAPH (May 13, 2017), http://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/.

116. *See* Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED (May 12, 2017), https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

117. Chris Graham, *NHS Cyber Attack: Everything You Need to Know About 'Biggest Ransomware' Offensive in History*, THE TELEGRAPH (May 20, 2017), http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

118. *Id.*

119. Although this is somewhat of an anomaly in recent years, even with the business industry having high profile data breach cases such as Target and Home Depot, *see* Khan, *supra* note 40, at 277 (citing the 2015 Ponemon Institute Study on the Cost of Data Breach Comprehensive Study). This number was derived from the total costs of data breaches over the number of records compromised.

120. *Id.*

121. *See* Ponemon Institute, *supra* note 63, at 1.

122. Elizabeth Snell, *Healthcare Data Breach Costs Highest for 7th Straight Year*, HEALTH IT SECURITY: PATIENT PRIVACY NEWS (June 20, 2017), https://healthitsecurity.com/news/healthcare-data-breach-costs-highest-for-7th-straight-year.

quadruple by 2019 to an estimated net cost of $2 trillion.[123] The costs for healthcare organizations goes beyond the dollar value of the EHRs compromised by cyber-attacks.[124] There are also indirect costs attached to every breach, including the use of organizational resources and the loss of goodwill.[125]

Patients suffer the most when healthcare organizations fail to adequately protect the sensitive information stored on their HISs. While patients often suffer some form of economic damage as a result of a data breach,[126] the greater—and often harder to measure—harm is from having their privacy violated.[127] Patients place their faith and trust in their healthcare providers. When this trust is broken or thrown into doubt because unauthorized individuals have accessed sensitive health information, it may be difficult to re-build. The non-monetary damage inflicted upon patients by data breaches is far more significant than the dollar value paid by healthcare organizations. Because of this, healthcare providers should work to their fullest extent to protect the data of their patients.

D. The Problem of Outsourcing

One problem that complicates the process of implementing safeguards to eliminate the risk of data security breaches is outsourcing. Outsourcing has been a staple across the information technology sector since the 1990s.[128] More recently, however, the healthcare industry has shifted larger portions of its resources abroad through outsourcing initiatives.[129] Doug Brown, the Managing Partner of the Black Book

123. *See* Dante Disparte & Daniel Wagner, *Do You Know What Your Company's Data is Worth?*, HARV. BUS. REV. (Sept. 16, 2016), https://hbr.org/2016/09/do-you-know-what-your-companys-data-is-worth.

124. *See* Khan, *supra* note 40, at 277.

125. *Id.*

126. For example, from unauthorized access to personal data, such as payment information (i.e. social security numbers, credit card numbers, etc.). In this regard, patients in healthcare data breaches suffer the same harm as consumers in large business data breaches. *See Cord Blood Bank Settles FTC Charges that it Failed to Protect Consumers Sensitive Personal Information*, FED. TRADE COMM'N (Jan. 28, 2013), https://www.ftc.gov/news-events/press-releases/2013/01/cord-blood-bank-settles-ftc-charges-it-failed-protect-consumers.

127. Privacy being a fundamental right. *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (holding that a penumbra of privacy is created by "several fundamental constitutional guarantees").

128. Kritika Bharadwaj, *How Safe is this Shore?—Data Protection and BPOs in India*, 27 J. MARSHALL J. COMPUTER & INFO. L. 539, 557 (2010).

129. *See* Black Book Market Research, *IT Outsourcing Booms in Healthcare Payer Sector as Insurers Go High Tech*, PR NEWSWIRE (Nov. 20, 2015), http://www.prnewswire.com/news-releases/it-outsourcing-booms-in-

Research Group, noted: "[H]ealth insurance niche software and service vendors are once again offering outsourcing as a cure-all for organizational cost controls."[130] Business process outsourcing companies (BPOs) are mostly a self-regulated industry.[131] While the HIPAA regulations offer no bright-line rule on offshoring, HIPAA is clear on the rules regarding business associates.[132] A business associate is a person or entity that "performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity."[133] But how does a healthcare provider ensure that offshore business associates are adequately protecting the ePHI of their patients?

III. RECOMMENDATIONS

Healthcare data security is clearly lacking. Despite the strides made by HIPAA thus far, it is far from perfect. This Part offers three primary modifications to HIPAA that would better protect patient ePHI stored on HISs while remaining scalable and flexible for the broad spectrum of healthcare organizations. This Part also briefly addresses the issues posed by outsourcing healthcare IT. Section III.A of this Note proposes mandating stricter technical safeguards for the protection of patient data. Section III.B offers a clearer and simplified guideline for compliance that incorporates industry best practices. Section III.C provides a framework that categorizes risks, which healthcare organizations would use to analyze the extent of the security measures they should reasonably use to maintain the flexibility that is central to HIPAA.

A. Mandate Stricter Technical Requirements

The technical safeguards provided by HIPAA are broad and fail to provide a clear guideline of what technical protections would be sufficient and what, at a minimum, should be required.[134] Encryption,

healthcare-payer-sector-as-insurers-go-high-tech-new-black-book-survey-300182354.html (finding that many health plans are budgeting at least 20% increases in outsourcing spends).

130. *Id.*

131. Bharadwaj, *supra* note 128, at 560.

132. *See* 45 C.F.R. § 164.502(e) (2007) (disclosures to business associates); *see also* 45 C.F.R. § 164.504(e) (2007) (requirements for business associate contracts).

133. *Business Associates*, U.S. DEP'T OF HEALTH & HUM. SERV. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (last updated Apr. 3, 2003).

134. *See*45 C.F.R. § 164.312 (2007) (listing all technical safeguards promulgated under the Security Rule).

for example, should be used whenever a healthcare organization deems it "appropriate."[135] The Security Rule mandates that healthcare organizations "[i]mplement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."[136] Not only is this extremely broad with little explanation, but it also only focuses on ePHI "being transmitted over an electronic communications network."[137] HIPAA does not mention electronic data storage standards.[138] A handful of specific, stricter technical safeguards would better protect patient data.

1. Require a 3-2-1 Rule for Data Backup

First, the Security Rule should be modified to better protect data through more efficient and stringent storage and backup requirements. Ideally, data backup plans should accomplish three things: (1) periodically and consistently backup data; (2) take special care regarding *where* the backup data is stored; and (3) avoid relying solely on online backup.[139] Requiring healthcare organizations to implement a 3-2-1 Rule for storing all ePHI would be ideal for achieving these objectives.[140] A 3-2-1 Rule is defined as a healthcare organization having "*three* copies of data, on *two* different types of media, with *one* of those copies being off site."[141] One of the types of media healthcare organizations should use must be external and offline. In addition to implementing a 3-2-1 Rule, healthcare organizations should be required to perform continuous data backup and recovery tests.[142] This would ensure that all copies of ePHI are up-to-date and that healthcare providers can be confident in their recovery systems.[143] HIPAA's Security Rule would benefit from requiring this data storage behavior in all healthcare organizations.

135. 45 C.F.R. § 164.312(e)(2)(ii) (2007).

136. 45 C.F.R. § 164.312(e)(1) (2007).

137. *Id.*

138. *See generally* 45 C.F.R. § 164.312 (2007).

139. Marion K. Jenkins, *The Top 5 Benefits of the HIPAA Security Rule*, PHYSICIANS PRACTICE (Mar. 30, 2011), http://www.physicianspractice.com/healthcare-careers/top-5-benefits-hipaa-security-rule.

140. *See* Dipshan, *supra* note 100.

141. *Id.* (emphasis added).

142. *See id.*

143. This will also important for already required provisions under the Security Rule's technical safeguards. For example, when a healthcare provider must access ePHI for an emergency under 160.312(a)(2)(ii) (2016).

This specific modification does not protect healthcare organizations by *preventing* ransomware attacks and other cybersecurity risks. What this data storage and backup behavior does is mitigate any damage to the healthcare provider caused by these types of attacks. Ransomware uses denial of access to important data as leverage to extort healthcare organizations.[144] Often times, the data held hostage is important to the healthcare provider's function in aiding its patients. For example, the data may include patient medical history and charts. Without it, doctors may not be able to adequately provide service to a patient. Following a ransomware attack, if healthcare organizations are able to address the cybercriminal's access point to their HIS, and then access the data that was held hostage, then they would no longer be pressured to pay the ransom. Healthcare organizations could instead take time to further analyze the situation and how to address the problem. If the organization properly addresses the access point the criminal used to encrypt the ePHI, then it may be assumed that the criminals no longer have access to the data. The healthcare organization would still, however, have to bear some cost in properly destroying the copy of the data that was encrypted by the cybercriminal if they cannot decrypt it without paying the ransom.[145]

2. Encryption

At a minimum, all healthcare organizations should be required to implement some level of encryption for highly sensitive ePHI. A simple symmetric key encryption should be used by all healthcare providers for all ePHI. Of course, if after performing the security management process, a healthcare organization discerns that its HIS contains a large store of patient ePHI, it may decide to use a public key encryption system or a hybrid encryption.[146] This would be more likely for larger healthcare systems, as opposed to smaller practices.[147] In conjunction

144. Kim Zetter, *What is Ransomware? A Guide to the Global Cyberattack's Scary Method*, THE WIRE (May 14, 2017), https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/ ("Ransomware is malware that locks your keyboard or computer to prevent you from accessing your data until you pay a ransom . . . ").

145. This may, or may not, be cheaper than the ransom demanded by the cybercriminal. That estimation would be on a case-by-case basis. Not paying the ransom, however, has the benefit of deterring the behavior of cybercriminals by not rewarding the criminal activity. *See Ransomware: Should You Pay the Ransom?,* EY ADVISORY (2016), https://advisory.ey.com/cybersecurity/should-you-pay-the-ransom.

146. *See* Katz, *supra* note 76, at 4-1.

147. Simply because larger healthcare systems, on the whole, have more resources and therefore a more sophisticated technology infrastructure. *See* Olin Bay, *Health Care Information Technology: A Key to Quality and*

with requiring encryption, the physical safeguards should be modified to mandate strict control of who within a healthcare organization has access to the key(s).[148] Only those that absolutely require access to patient ePHI should have access to the key(s). This may also be helpful when sending ePHI within a network from one organization member to another through the use of a public key encryption system. Finally, one thing all healthcare organizations should be required to do is to occasionally re-encrypt ePHI.[149] Each healthcare organization may analyze their needs and the risks involved to decide how frequently this is done, but creating new key pairs should be done at least every five years.

Encryption comes with several potential challenges. What if a malicious employee with access to a key is terminated? Must a healthcare organization pay for revoking the key and ciphertext to re-encrypt the ePHI? What about cloud storage—where data is stored in logical pools as opposed to on physical devices—which is increasingly used in the healthcare industry?[150] Access control is a major issue, both inside and outside the growing field of cloud data storage.[151] One developing solution is self-updatable encryption, in which the ciphertext and a private key are directly correlated to a period of time.[152] A person within an organization may then be able to decipher data only within the time limit

Cost Issues, LEAGUE WOMEN'S VOTERS (2010), http://www.montrose.co.lwvnet.org/files/hcet_bp_healthcareinfotech.pdf.

148. *See generally* 45 C.F.R. § 164.310 (2007) (physical safeguards control personnel access to facilities and workstations, an addition can be made that functions very similarly for decryption keys).

149. This is fairly easy to do. Take, for example, re-encryption and key rotation for Google's Cloud KMS. *See*, *e.g.*, *Key rotation*, GOOGLE CLOUD PLATFORM, https://cloud.google.com/kms/docs/key-rotation (last updated June 26, 2017) (showing re-encryption and key rotation for Google's Cloud KMS). *See also Re-encrypting Data*, GOOGLE CLOUD PLATFORM, https://cloud.google.com/kms/docs/re-encrypt-data (explaining that the process for re-encrypting data is fairly straightforward and involves decrypting the data, using a new primary key to re-encrypt the data, and then disposing of the prior used key).

150. *See* Iron Mountain, *Cloud Data Storage: Why Healthcare Organizations are Taking Notice*, IRON MOUNTAIN KNOWLEDGE CTR., http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/General-Articles/C/Cloud-Data-Storage-Why-Healthcare-Organizations-Are-Taking-Notice.aspx (last accessed Mar. 4, 2017) ("Nearly one-third [73%] of healthcare decision makers said they are using cloud applications").

151. *See* Kwangsu Lee, et al., *Self-updatable Encryption: Time Constrained Access Control with Hidden Attributes and Better Efficiency*, 667 THEORETICAL COMPUTER SCIENCE 51, 52 (2017).

152. *Id.* at 52

that their key works.[153] This type of encryption system may also provide cloud data servers with a comforting level of access control and security.[154]

Encryption, much like mandating a 3-2-1 Rule, does not directly prevent ransomware attacks. It primarily protects patients by making any ePHI a cybercriminal may access indecipherable, and thus incapable of being used to harm patients. Unlike the 3-2-1 Rule, encryption and its strategic use may limit the risk of cybersecurity breaches by limiting the flaws in the protections of HISs. An encrypted HIS is less likely to fall victim to non-technical methods of penetration, such as breaches resulting from human error or deviance.[155] Encryption may also deter cybercriminals across the board, as the data has little value if it is in indecipherable ciphertext.[156]

3. Data-at-rest v. Data-in-motion

HIPAA should provide differentiated requirements for data-at-rest and data-in-motion. Data-at-rest means data that is stored in some static form.[157] For example, the data in file systems and databases are data-at-rest.[158] Data-in-motion means data "as it moves through the network to the outside world."[159] Data that is in transit via e-mail, messaging software, peer-to-peer (P2P) networks, or any similar mechanisms are examples of data-in-motion.[160] To adequately protect sensitive data, data-at-rest must be treated differently from data-in-motion.[161] The safeguards this Note proposes for data-at-rest generally involves software protections and cyber hygiene. On the other hand, data-in-motion requires a level of authentication. Both types of data should be encrypted.

153. *Id.* at 57.

154. *Id.* at 51.

155. *See* Robert Lemos, *Use Data Encryption to Safeguard your Data*, PC WORLD (Nov. 13, 2008), http://www.pcworld.com/article/153826/data_encryption_tools.html.

156. *Id.*

157. *See* Simon Liu & Rick Kuhn, *Data Loss Prevention*, 12 IT PROFESSIONAL 10, 11 11 (2010), http://csrc.nist.gov/groups/SNS/rbac/documents/data-loss.pdf.

158. *Id.*

159. *Id.* at 12.

160. *Id.*

161. *Id.* ("Data in each state often requires different techniques for loss prevention. For example, although deep content inspection is useful for data in motion, it doesn't help so much for data at rest.").

HIPAA should require a minimum level of organizational cyber hygiene and resilience.[162] HIPAA should explicitly require that organizations implement endpoint security protections, intrusion-prevention software, and web browser protection for all devices with accessibility to both an HIS and the internet. Further, it should require that all healthcare organizations update their software. The period of time between software updates should be, at a minimum, weekly, though healthcare organizations may determine this need on a case-by-case basis. HIPAA should also be modified to require penetration testing. This means that an IT security company evaluates the security of an organization's security infrastructure.[163] These tests highlight vulnerabilities not only in protective software, but in system configuration and end-user behavior.[164] The frequency and extent of these penetration tests would depend on the size and capabilities of the healthcare organization.[165] Organizations would determine this after performing their own risk assessments.

Healthcare organizations should also take measures to secure ePHI that is in motion, either across a HIS or that is travelling to an external location. While the most effective method of protection is encryption, there are other steps that healthcare organizations could *and* should take. HIPAA should mandate that healthcare organizations implement technical policies and procedures for both data-in-motion and data-at-rest. As an addressable implementation specification, HIPAA should require that healthcare organizations use *both* authentication and a virtual private network (VPN). Authentication would ensure that all data being sent and received is either going to or coming from a trusted source.[166] This would prevent many of the tactics cybercriminals use to infiltrate HISs and begin ransomware schemes.[167] All ePHI sent from a

162. The concept of cyber hygiene refers to the responsibility of *individuals* to maintain the "health" of the user's system. It is centered on routine and contributes on a organizational level to cybersecurity. *See* Floyd McKinney, *Fight Security Decay; Cyber Hygiene*, ENGILITY (Sept. 17 2017), https://www.engilitycorp.com/blog/article/fight-security-decay-practice-good-cyber-hygiene.

163. *See What is Penetration Testing?*, CORE SECURITY, https://www.coresecurity.com/penetration-testing-overview (last visited Oct. 22, 2017).

164. *Id.*

165. *Frequently Asked Questions*, HALOCK SECURITY LABS, https://www.halock.com/frequently-asked-questions-pages-357.php (last visited Oct. 23, 2017).

166. *See, e.g.,* Lily Hay Newman, *If You Want a VPN to Protect Your Privacy, Start Here*, WIRED (Mar. 30, 2017), https://www.wired.com/2017/03/want-use-vpn-protect-privacy-start/

167. Because VPNs secure peer-to-peer networks, this method would limit phishing e-mails that appear to come from an internal source (and thus more likely to be opened by the victim). 7 *Steps to Protect Yourself*

secured network environment should only be received through the use of a VPN because a VPN creates "a secure connection even on a public unsecured network."[168] This is a particularly important option for mobile devices used to access or transmit ePHI.[169] Requiring healthcare organizations to implement or consider implementing some form of these measures would protect patient ePHI from ransomware and other cybersecurity attacks.

4. Prohibit Use of Generic Usernames

The Security Rule's technical safeguards require healthcare organizations to "[a]ssign a unique name and/or number for identifying and tracking user identity."[170] This, unfortunately, is not enough. This provision should be modified to explicitly prohibit the use of generic passwords for any device or workstation operated by a healthcare organization. Also, there should either be a prohibition against commonly shared work stations, or at the very least strict controls regarding these workstations. The Recommended HIPAA Security Standards developed by the University of South Florida's (USF) HIPAA Security Team, for example, provides a more stringent version of the Unique User Identification Standard.[171]

USF's recommended standard prohibits both generic usernames and passwords. Furthermore, their recommended standard explicitly sets a minimum quality requirement for passwords.[172] Under their recommended standard: "Passwords are to consist of at least six characters, and should include alpha, numeric, *and* special characters in order to prevent unauthorized password use or password guessing."[173] This standard, or something similar to it, should be required to prevent blunt force breach attempts. USF's standard, unlike the one currently promulgated by HIPAA, also addresses common work stations.[174] Where multiple users

Against Corporate Spear Phishing, LINOMA SOFTWARE (June 28, 2017), https://www.goanywhere.com/blog/2017/06/28/7-steps-to-protect-yourself-against-corporate-spear-phishing.

168. *See Use Adequate Security to Send or Receive Health Information Over Public Wi-fi Networks*, HEALTH IT, https://www.healthit.gov/providers-professionals/10-use-adequate-security-send-or-receive-health-information-over-public-wi-f (last updated Mar. 21, 2014).

169. *Id.*

170. 45 C.F.R. § 164.312(a)(2)(i) (2007).

171. *See* HIPAA Security Rule Safeguards Recommended Standards, UNIV. S. FL. (May 12, 2005), http://health.usf.edu/nr/rdonlyres/2d58eb73-e08a-4ede-b3bf-2ef77a4ad70c/0/usfhipaasecurityrulestandards.pdf.

172. *Id.* at 8.

173. *Id.* (emphasis added).

174. *Id.*

are required to have access to one workstation, USF still requires stringent access to the individual applications on the workstation.[175] USF's recommended standards for user identification are a great example of what HIPAA should require of all healthcare organizations. Heightened access standards like these should be paired with personnel limitations on access to certain parts of HISs to generally protect against negligently introducing malware and cybersecurity attacks, including ransomware.

5. Require Access-Triggered Breach Notification

Under HIPAA's Breach Notification Rules, healthcare providers are required to notify individuals "whose [ePHI] has been, or is reasonably believed . . . to have been accessed, acquired, used, or disclosed as a result of such breach."[176] This seems sufficient on its face. Unfortunately, under the same rule, unauthorized access is not a breach if a healthcare provider determines "that there is a low probability that the protected health information has been compromised based on a risk assessment."[177] The factors of the risk assessment include "whether the [ePHI] was actually acquired or viewed."[178] As a result, cybersecurity breaches such as ransomware attacks, where the data is encrypted, would not trigger notification to individuals. Therefore, despite the organization's HIS being penetrated and the data being "accessed" by an unauthorized person, patients are left in the dark about whether their ePHI is involved or not.

HIPAA's data breach notification should be revised to replace the "risk assessment" with an automatic access-based trigger. This means that notification would be triggered "whenever personal data is reasonably believed to have been acquired by an unauthorized person and require no evidence that an unauthorized person actually acquired the data."[179] A ransomware attack and similar breaches should then satisfy this requirement. Transparency is important and therefore whenever there is a reasonable belief of unauthorized access, patients should be kept informed of potential risks involving their sensitive personal information.

An argument against such a modification is that patients would be overwhelmed with notifications and de-sensitized to the notices that

175. *See id.*

176. 45 C.F.R. § 164.404(a)(1) (2016).

177. 45 C.F.R. § 164.402(2) (2016).

178. *Id.*

179. Stanley C. Ball, Note, *Ohio's "Aggressive" Attack on Medical Identity Theft*, 24 J.L & HEALTH 111, 138 (2011) (The student-author in this Note focuses on state law in the context of medical identity theft, the definition used is nevertheless helpful here.).

healthcare organizations send out.[180] This is problematic if patients are unable to decipher when a breach is particularly important (i.e. when their personal data has actually been acquired and the risk of medical or financial identity theft is realistic). First, if data stored in HISs are properly encrypted, then that eliminates the need to not provide notice at all. This is because breaches under HIPAA only involve unsecured ePHI.[181] Through the use of encryption, the data are rendered unusable, unreadable, and indecipherable.[182] Second, to further address this issue, the *type* of notice provided should be based on a factor-based risk analysis. Currently, HIPAA requires written notice for individual notification.[183] Without actual proof of access or acquisition of data, the form of notice should be online and easily accessible to patients. Patients should, however, be occasionally reminded of the existence of these postings. For breaches where individuals' data are acquired by unauthorized persons, written notice should be provided as it is currently laid out in the federal regulations.[184]

B. Provide Clearer & Simplified Compliance Guidelines

In their 2007 article, Professors Sharona Hoffman and Andy Podgurski argue in part that one of the flaws of HIPAA's Security Rule is that, in providing covered entities with flexibility and discretion, the Rule fails to provide adequate guidance on *how* the covered entities should comply with the requirements.[185] The authors also contend that "some organizations could use the regulations' vagueness as a justification for establishing minimal PHI security measures."[186] Finally,

180. *See Experts Forecast Top Seven Trends in Healtcare Information Privacy for 2011*, IDEXPERTS (Jan. 05, 2011), https://www2.idexpertscorp.com/knowledge-center//single/experts-forecast-top-seven-trends-in-healthcare-information-privacy-fo . Or this leaves patients simply terrified all the time. *See* Asha Saxena, *6 Ways Hospitals Can Ease Patients Fears About Security Threats*, BECKER'S HEALTH IT & CIO REVIEW (May 26, 2015), https://www.beckershospitalreview.com/healthcare-information-technology/6-ways-hospitals-can-ease-patients-fears-about-security-threats.html.

181. 45 C.F.R. § 164.404(a)(1) (2016) ("A covered entity shall, following the discovery of a breach of *unsecured* protected health information . . . ") (emphasis added).

182. *See* 45 C.F.R. § 164.402 (2016) (defining "unsecured protected health information").

183. 45 C.F.R. § 164.404(d)(1) (2016).

184. *See, e.g., id.*

185. Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 BOS.C. L. REV. 331, 350-51 (2007).

186. *Id.* at 351.

they point out that the Security Rule does not require that healthcare organizations rely on the "best current security practices" of the data security community.[187] One of the "reputable organizations" that the authors recognize as a potential basis for "best practices" in complying with HIPAA Security is the National Institute of Standards and Technology (NIST).[188]

HHS should officially adopt NIST's data security standards as best practice for the entire healthcare industry. NIST and HHS already have a long history of working closely together, so promoting NIST in the federal regulations would not be a sweeping change.[189] Healthcare organizations should be required to perform their risk assessments in light of the standards promoted and drafted by NIST. For example, healthcare organizations should refer to the NIST risk management framework (RMF).[190] The RMF provides a "disciplined, structured, extensible, and repeatable process for achieving risk-based protection related to the operation and use of information systems."[191] All healthcare organizations should follow and apply the RMF when complying with the Security Rule.

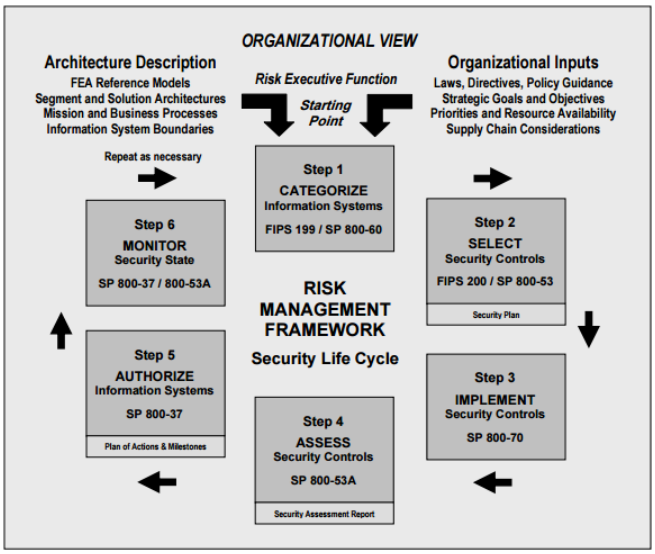
187. *Id.* at 252–3.

188. *Id.*

189. *See, e.g., Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework,* U.S. DEP'T OF HEALTH & HUM. SERVS. https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html?language=es (last updated Feb. 23, 2006). The "crosswalk" identifies points of interaction between the Security Rule and NIST Framework, as well as other widely known security frameworks.

190. *See* NATL' INSTITUTE OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, SP 800-66 REV. 1, AN INTRODUCTORY RESOURCE GUIDE FOR IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) SECURITY RULE, 10 (Oct. 2008), *available at:* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf [hereinafter Scholl].

191. *Id.; see also* Figure 3.



192

Figure 3.[193]

As NIST has pointed out, the RMF overlaps with the implementation standards promulgated under the Security Rule. The six steps distill much of the spirit of the Security Rule into an easy to follow process. In conjunction with the six-step RMF, NIST has also provided questions to help guide compliance with the Security Rule's three general safeguards.[194] Providing an explicitly adopted best practice standard for complying with the Security Rule helps ensure that healthcare organizations implement sufficient measures to protect against cybersecurity threats, including ransomware.

C. A Flexible Administrative Standard

One of HIPAA's policy goals was to provide healthcare organizations with flexibility and discretion in applying it's mandates.[195] A small-town private practice with a single physician, for example, would not apply the same level of security measures as a national hospital network. Along with using NIST as an understandable basis for complying with HIPAA, the flexibility standard should be revised so that healthcare organizations may retain flexibility but do not have too much discretion as to apply minimal standards in some cases.

192. Scholl, *supra* note 190, at 11 ("Many Security Rule standards and implementation specifications correspond to the steps of the NIST RMF.").

193. *Id.* at 11. (showing a visual portrayal of the NIST Risk Management Framework.).

194. *See id.* at17–53.

195. *See* 45 C.F.R.§ 164.306(b) (2016) (flexibility of approach).

There are many registers of information technology security threats.[196] HHS should develop and maintain a similar database that documents cyber-threats to e-PHI and HISs, borrowing from already existing registers while contributing healthcare-specific threats. These threats should be categorized into three risk groups: known, semi-known, and unknown.[197] Known threats are those that are clearly known and can easily be addressed through implementing clearly defined technical safeguards.[198] These threats include malware that has been identified, is widely known, and up-to-date endpoint protection software would adequately protect against.

Semi-known threats are threats that "the cybersecurity industry has already identified [many of the risks for and] . . . best practices for addressing them."[199] Unlike known threats, there is no clear solution to semi-known threats and best practices to address related risks are not commonly implemented throughout the industry. These threats include ransomware. For example, there is no common solution to ransomware once an organization's data is encrypted. While broadly accepted preventative measures are promoted by experts, there is no clear solution to thwarting ransomware. Also, healthcare organizations must still calculate the "likelihood and magnitude" of these types of threats.[200] All healthcare organizations should protect themselves against known threats, and in some way address semi-known threats.

Finally, only healthcare organizations with sizeable HISs and mature, well-developed security capabilities and culture should in any way address unknown threats. Unknown threats "represent failures of imagination."[201] Therefore, only organizations with a developed technology infrastructure have the luxury, time, and resources for dealing with this kind of non-immanent threat. The few, capable organizations should make habitual inquiries into cybersecurity and address potential, yet-to-be identified threats by foreseeing potential liabilities in their use

196. *See, e.g., Security Response Center*, SYMANTEC https://www.symantec.com/security_response/ (last visited Oct. 22, 2017) (Symantec lists and categorizes every cyber-threat and continually updates this list).

197. *See* Noah G. Susskind, Note, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & BUS. 573 (2015). This tripartite structure was influenced by a similar idea proffered by the student-author here. Unlike this Note, however, this author focuses on the financial industry and corporate governance and management, where I apply a similar idea to the healthcare industry and HIPAA. The idea of applying this tripartite to a register of threats is also unique to this Note.

198. *Id.*

199. *Id.* at 601.

200. *Id.*

201. *Id.* at 618.

of IT in relation to their HISs. This tripartite structure for flexibility in administering security safeguards strikes a balance between allowing healthcare providers to have discretion and more stringently protecting patient ePHI.

D. Addressing the Outsourcing Problem

If a large-scale data breach involving ePHI were to happen offshore where a vendor performs outsourced services, it is unclear what the ability of HHS would be to enforce HIPAA against the offshore organization. Currently, HIPAA mandates what disclosures a covered entity may make *to* business associates (BAs) and what disclosures BAs may in turn make.[202] It does not, however, clearly identify offshore service providers as BAs. Kirk Nahra, chair of Wiley Rein LLP's Privacy Practice, when asked about whether offshore vendors constitute business associates under HIPAA, had to say, "HIPAA doesn't say a word about offshore. But a BA is a BA is a BA."[203] On the bright side, India's laws and self-regulation standards are comforting for any person worried about the security of ePHI handled by offshore vendors located in the country.[204] The India Information Technology Act of 2008, modified in 2011 by the Information Technology Rules, mandates strict requirements for the privacy of sensitive data.[205] These rules include the requirement that organizations collecting personal data "must have in place reasonable security practices and procedures."[206] Indeed, it is likely that many offshore vendors "with a history of dealing with U.S. health-care clients—are as good or better than U.S. companies at protecting data."[207] Still, HIPAA should be further modified to include vetting criteria for covered healthcare organizations thinking of outsourcing services overseas.[208]

---

202. *See* 45 C.F.R. § 164.502(e) (2016).

203. *Kirk Nahra Discusses HIPAA Compliance Questions Involving Offshore Vendors,* WILEY REIN LLP (Aug. 14, 2013), http://www.wileyrein.com/newsroom-media-992.html [hereinafter Wiley Rein].

204. *See* Todd B. Ruback & Sarah Mahony, *An Overview of Recent Statutory Changes to Privacy Law in India in Comparison to Similar U.S. and EU Privacy Rules*, 2011 N.J. LAW. 38, 40 (2011).

205. *Id.*

206. *Id.*

207. *See* Wiley Rein, *supra* note 203 (quoting Kirk Nahra).

208. I leave this proposition with the question. While I do not believe outsourcing is a major issue for this topic as of now, I do think this proposal is one worth more thought. For the sake of brevity, however, I will save it for later discussion. *See generally, After OCR Probe of Stolen Flash Drive, Hospital Is Not Fined; Upgrade Was Under Way*, REP. ON MEDICARE COMPLIANCE (Feb. 27, 2017), https://www.kslaw.com/attachments/000/004/735/original/rmc_feb_27-2.pdf?1499727809.

IV. THE FEDERAL TRADE COMMISSION

Even if HIPAA is not modified, the practices proposed in this Note should be adopted by all healthcare organizations as industry best practices. Healthcare organizations should adopt these proposals because inadequately safeguarding patient data despite clear evidence of cyber-threats across the industry may mean liability for unfair practices towards their patients. This Part explains the recently developing history of Federal Trade Commission (FTC) enforcement of data security practices and the FTC's authority over this subject matter. In the most recent case of *LabMD*, the FTC developed a legal framework for liability that makes many healthcare organizations liable for poor data security practices, even when no actual harm occurs to their patients as a result. The FTC's recent actions afford a strong impetus for healthcare providers to make these proposed modifications.

A. FTC v. Wyndham Worldwide Corp.

The FTC has played a strong role in enforcing cybersecurity cases since the early 2000s. On January 31, 2014, the FTC announced the milestone of its fiftieth data security settlement.[209] The FTC further solidified its position as the authority of the data security field by releasing its own guidance on the subject.[210] The FTC's enforcement was challenged and affirmed in the case *FTC v. Wyndham Worldwide Corp.*.[211] There, Wyndham challenged the FTC's statutory authority to regulate data security practices after the FTC filed suit against Wyndham alleging unfair and deceptive practices for data breaches occurring between 2008 and 2014.[212] The district court found for the FTC, holding that it possessed the requisite authority to enforce data security claims.[213]

The data breaches resulted in hackers obtaining payment information—including credit card numbers and security codes—of over 600,000 consumers, resulting in $10.6 million in fraud loss.[214] The hackers infiltrated property management systems that process

209. *See* FED. TRADE COMM'N, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

210. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

211. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

212. *See id.* at 241.

213. *Id.* at 631.

214. *Wyndham Worldwide Corp.*,799 F.3d at 242.

consumer information that Wyndham managed.[215] The FTC alleged that as far back as 2008, Wyndham managed these systems in a manner that "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[216] This included: (1) storing payment information in clear, readable text; (2) using "easily guessed" passwords to secure the management systems; (3) allowing the management systems to connect to Wyndham's entire network without appropriate technical precautions[217]; (4) failing to "adequately restrict" the access of third-party vendors to the network; and (5) not following proper procedure or conducting an investigation following a security breach.[218]

The Federal Trade Commission Act (FTC Act) prohibits "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive practices in or affecting commerce."[219] The U.S. Court of Appeals for the Third Circuit pointed out that Congress designed the term "unfair methods of competition" as a flexible concept and left its development to the FTC.[220] The FTC provided guidance on factors governing unfairness determinations, which the Supreme Court later adopted:

> (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy . . . whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness;
>
> (2) whether it is immoral, unethical, oppressive, or unscrupulous; and
>
> (3) whether it causes substantial injury to consumers.[221]

215. *Id.* at 241.

216. *Id.* at 240.

217. For example, Wyndham allowed at least one hotel to connect to its system with a security system that had not been updated in three years. Wyndham also permitted connection with the use of default usernames and passwords.

218. *Wyndham Worldwide Corp.*,799 F.3d at 240–241.

219. 15 U.S.C. § 45(a)(1) (2006); *see also* 15 U.S.C. § 45(n) (2006) ("The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves.").

220. *Wyndham Worldwide Corp.*,799 F.3d at 243.

221. *Id.*

The appellate court affirmed the district court's decision.[222] Wyndham also argued that the FTC's claim should fail because its conduct was not unethical or unscrupulous, and because a business "does not treat its customers in an 'unfair' manner when the business 'itself' is victimized by criminals."[223] The court rejected both arguments, holding that unfairness claims may be brought on *likely* rather than actual injury.[224]

B. In re LabMD

The FTC's authority in the realm of data security was extended in the case of *LabMD*. In July 2016, the FTC heard a case regarding the negligent handling of sensitive patient information by a medical testing company.[225] LabMD—the company in question—provided management employees with administrative rights over their workstations (i.e. control over their workstation's operating system), including sales employees.[226] Around 2005, LabMD's billing manager and others in the department accidentally exposed files containing sensitive patient data to a P2P file-sharing program.[227] Later, unauthorized persons accessed a file containing these sensitive health data, which included names and social security numbers of 600 patients.[228]

The FTC overturned an administrative law judge (ALJ)'s ruling where the ALJ defined the phrase "'likely to cause [substantial injury]'" to mean "'having a high probability of occurring or being true.'"[229] The ALJ also held that the unauthorized exposure of sensitive medical data, without an accompanying tangible injury, fell outside the scope of "substantial injury" under the FTC Act.[230] Looking to the *Wyndham Worldwide* three-part test, the FTC found that LabMD failed to: protect its computer network with even the most fundamental cyber hygiene practices; provide data security training to its employees; and restrict or monitor the computer practices of persons using its network.[231]

222. *Id.* at 259.

223. *Id.* at 246.

224. *Id.*

225. *See In the Matter of LabMD, Inc.,* 2016 FTC LEXIS 128 *1 (F.T.C. July 28, 2016)

226. *Id.* at *4–5.

227. A P2P file-sharing program is one that allows the sharing of media files through the use of a peer-to-peer network., *id.* at *5.

228. *Id.* at *11.

229. *Id.* at *56.

230. *In the Matter of LabMD, Inc.,* 2016 FTC LEXIS at *19.

231. *See id.* at*9–10.

The panel of commissioners of the FTC held that the FTC could act preemptively and without a showing of tangible harm.[232] The FTC also found that while cases of unfairness usually involve tangible, economic harm, the FTC Act recognized other forms of harm.[233] Therefore, in concluding that LabMD's security practices were unreasonable and lacked "even basic precautions," the FTC held that actual harm is not necessary for a finding of "unfair" conduct.[234] Organizations can be liable if their practices create a *risk* of harm and negligent security practices were sufficient to create liability for data security breaches.[235]

C. FTC on the Move

The FTC has recently focused its data security guidance and enforcement on the threat of ransomware. FTC Chairwoman Edith Ramirez publicly announced that "[a] company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the FTC Act."[236] The FTC has also issued guidance on the topic of ransomware-prevention.[237] Within this guidance, the FTC lays out what it minimally expects of organizations to defend against ransomware attacks:

> (1) Implement education and awareness programs to train employees to exercise caution and avoid phishing schemes;
>
> (2) Practice good security by implementing basic cyber hygiene principles;
>
> (3) Back up data early and often; and
>
> (4) Develop and test incident response and business continuity plans.[238]

232. *Id.* at *68.

233. *Id.* at *72.

234. *Id.* at *1.

235. *Id.* at *62–63; *but see* LabMD, Inc. v. FTC, 678 F. App'x 816, 822 (11th Cir. 2016) (circuit court granting stay pending appeal in favor of LabMD on order requiring LabMD to implement data security compliance measures).

236. *See* Cara Salvatore, *FTC Chair Threatens Action On Ransomware Holes*, LAW360 (Sept. 8, 2016), https://www.law360.com/articles/837883/ftc-chair-threatens-action-on-ransomware-holes.

237. Ben Rossen, *Ransomware: a Closer Look*, FED. TRADE COMM'N, (Nov. 10, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look.

238. A lot of these practices that the FTC urges organizations to invest in are consistent with the technical recommendations offered in this Note, *see id.*

The FTC has also supported the use of standards promulgated by NIST and the use of NIST's security framework.[239] In fact, the FTC has concluded that the NIST framework and the FTC's data security approach are "fully consistent."[240] Because of the relationship that exists between HHS and the FTC,[241] and the FTC's stance on and response to unreasonable data security practices, FTC enforcement may create a lot of issues for healthcare organizations.

D. Implications for Healthcare Providers

In light of the FTC's decision in *LabMD* and its strong stance on ransomware protections, healthcare organizations have a strong impetus to make modifications to their HIS data security. While there is no private cause of action under HIPAA,[242] OCR enforces HIPAA's Security Rule.[243] This enforcement process involves a complaint, a subsequent investigation, followed either by a resolution from OCR or a criminal violation that the DOJ will pursue.[244] Now, the FTC may hold healthcare organizations personally liable for unfair and deceptive practices towards their patients for poor data security practices.

First, ransomware presents a clear case of risk of harm, as opposed to actual harm. The fact that an unauthorized person accesses a HIS makes the substantial harm *likely*, which is sufficient for FTC action. Although no tangible economic harm may occur to patients for the intrusion of ransomware, the access to their ePHI is enough to create an unfair practice under the FTC Act. Second, because of recent ransomware attacks, all healthcare organizations are aware of the threat and how the attacks are typically carried out. Failing to take adequate preventative measures would be equivalent to Wyndham's and LabMD's negligent practices. Finally, the potential harm caused to

239. *See* Andrea Arlas, *The NIST Cybersecurity Framework and the FTC,* FED. TRADE COMM'N (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.

240. *Id.* ("The types of things the Framework calls for organizations to evaluate are the types of things the FTC has been evaluating for years in its Section 5 enforcement to determine whether a company's data security and its processes are reasonable.").

241. *See, e.g., Sharing Consumer Health Information?*, U.S. DEP'T OF HEALTH & HUM. SERV.(Oct. 2016)https://www.hhs.gov/hipaa/for-professionals/special-topics/HIPAA-ftc-act.

242. 45 C.F.R. § 160.300-.552 (2016) (covering the enforcement process under HIPAA); *see also* FRANCOISE GILBERT, *Enforcement*, in A GUIDE TO HIPAA SECURITY AND THE LAW 101, 107-108 (Stephen S. Wu, ed., 2007).

243. *See Enforcement Process*, U.S. DEP'T OF HEALTH & HUM. SERV. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html (last updated June 7, 2017).

244. *Id.*

patients is not reasonably avoidable by patients themselves. Unless healthcare providers wish to face the same consequences as these companies, they should take the appropriate steps to protect the data of their patients from ransomware, as well as other known and emerging threats. Thus, even if HIPAA is not amended, healthcare organizations should take action in light of potential FTC enforcement.

V. CONCLUSION

Sweeping changes to HIPAA's Security Rule are impracticable and unnecessary. Specific modifications—as proposed in this Note—would better carry out HIPAA's purpose to protect the privacy of patient ePHI from unauthorized persons. These proposed changes protect the data from unauthorized access in particular. New threats, such as ransomware, arise and expose chinks in the armor that HIPAA's Security Rule supposedly placed over the body of ePHI, making the need for these changes increasingly clear. These proposed modifications would provide a heightened level of security while remaining flexible, as healthcare organizations all have different needs, capabilities, and budgets. While these changes would be beneficial, there is no single or perfect answer to the question of how to protect patient data in this digital world and digital economy. HIPAA should be modified for the benefit of patients, whose private and valuable information is held in trust by healthcare organizations. And even if these modifications are not adopted, healthcare organizations should act to better protect their patients' data.